COSIC

KU LEUVEN

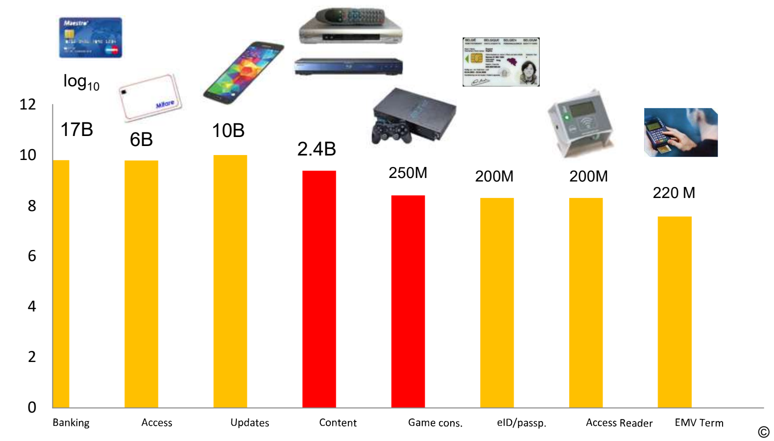
The Quantum Threat and Post-Quantum Cryptography (PQC)

Bart Preneel
COSIC KU Leuven
Bart.Preneel(at)esat.kuleuven.be @bpreneel1
4 June 2024

1

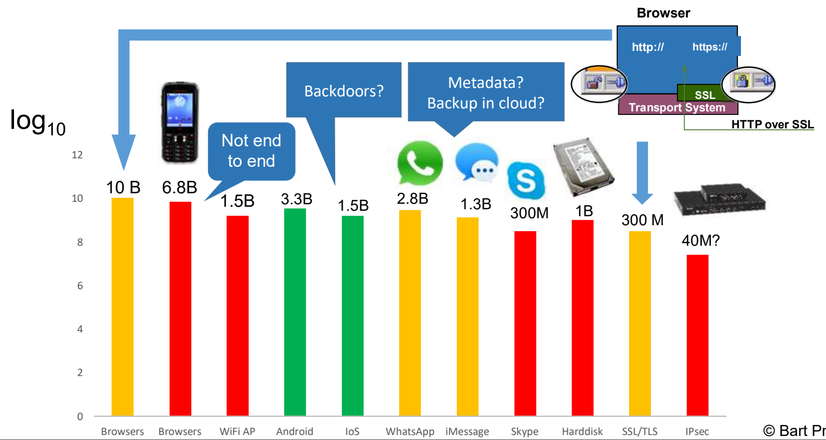
1

Cryptography to protect industry ~35 B



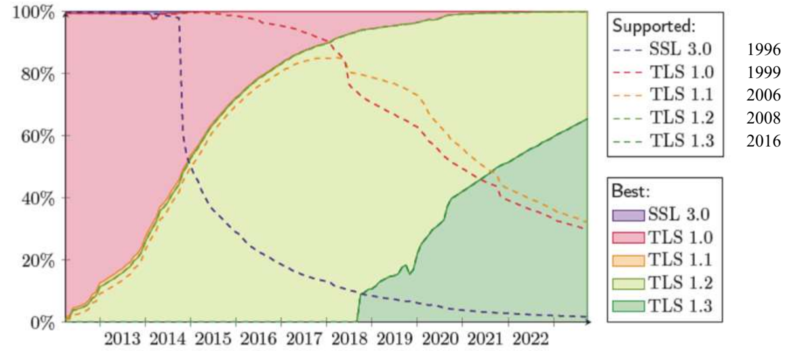
2

Cryptography to protect user data ~28 B



3

TLS migration on top 150K websites



Source: https://www.ssllabs.com/ssl-pulse/

4

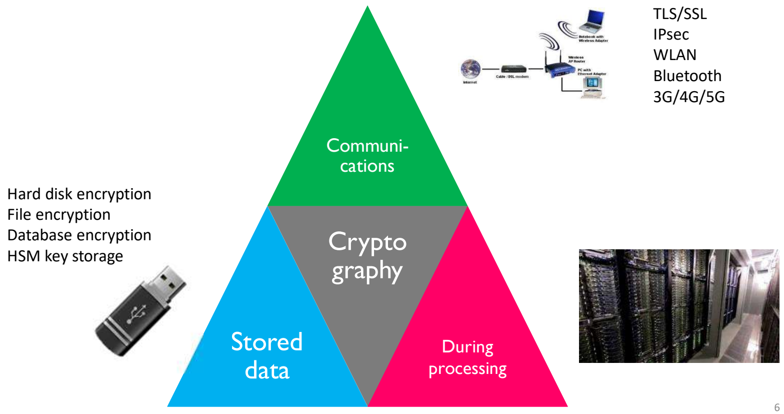
"Advanced" cryptography at scale

- TPM: anonymous credentials
- Intel SGX for private contact discovery in Signal
- Message franking: committing AEAD
- (Partially) Oblivious PRF: breaches password checking
- Cryptocurrencies:
  - Monero (ring signatures)
  - Zcash (ZK-SNARK)
  - Ethereum ZK-rollups (layer 2)

5

5

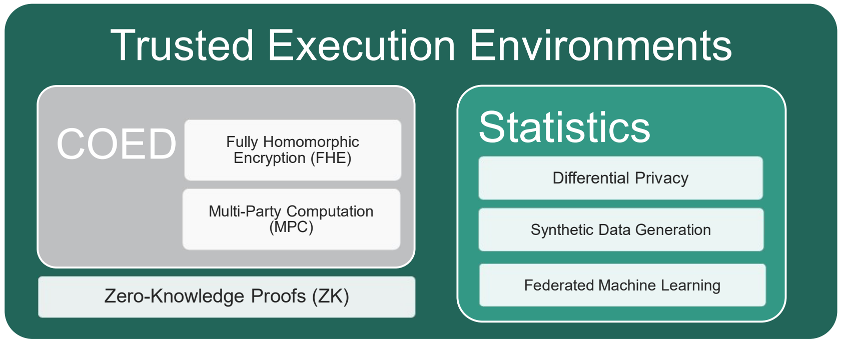
Changing role of cryptography



6

6

Computing on Encrypted Data (COED)



KU LEUVEN

7

Outline

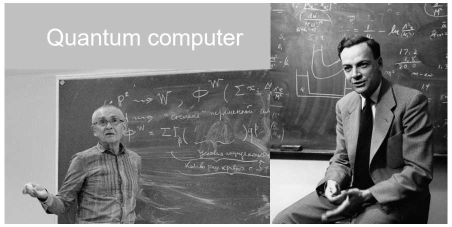
- Quantum computers and impact on cryptography
- The NIST competition: focus on public-key encryption
  - digital signatures: see tutorial of Ludovic Perret
- Migration issues

8

8

The advent of quantum computers

Yuri Manin 1980
Richard Feynman 1981
Exponential parallelism



Jan. 2014: NSA has spent 85 M$ on research to build a quantum computer

9

9

If a large quantum computer can be built

public-key cryptography algorithms have to be replaced [Shor'94]
RSA, Diffie-Hellman (including elliptic curves)

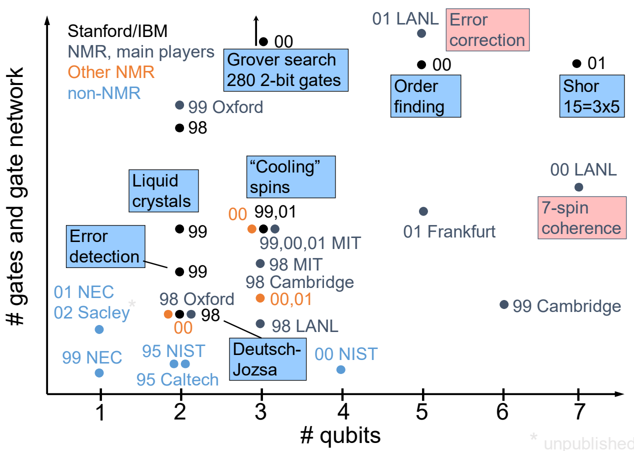
Breaking RSA-2048 requires 4096 ideal qubits or 20 million real qubits

symmetric crypto: key sizes: x2 [Grover'96]
but huge quantum devices needed

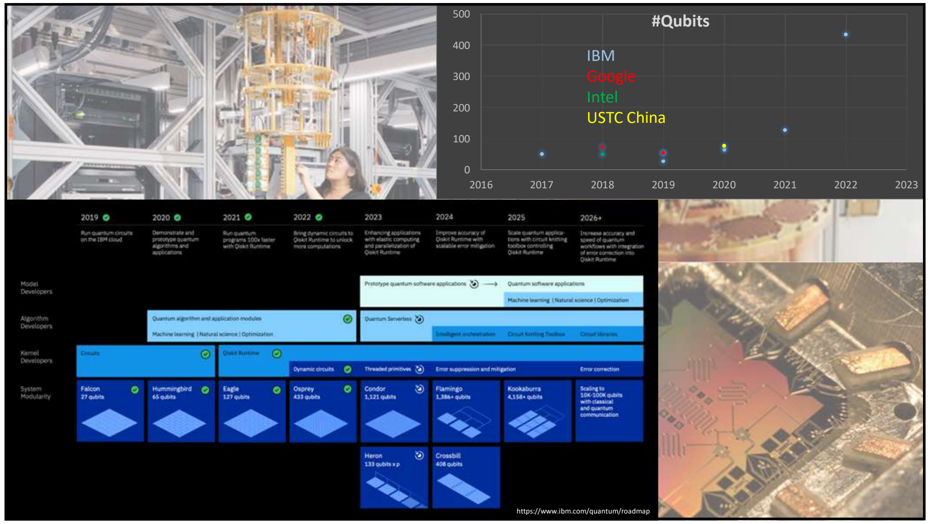
10

10

State of the art in coherent qubit control ('01)



11

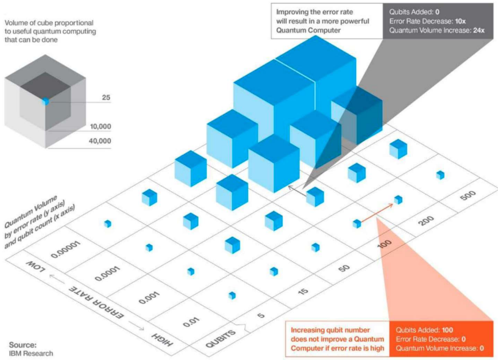


12

It's not only about qubits: error rate

Quantum Volume

IBM



© 2017 IBM

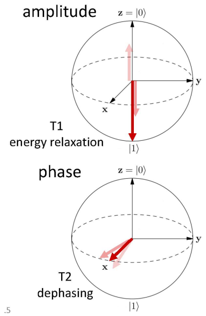
13

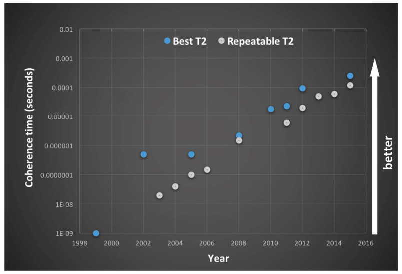
It's not only about qubits: decoherence

decoherence

loss of quantum information

IBM



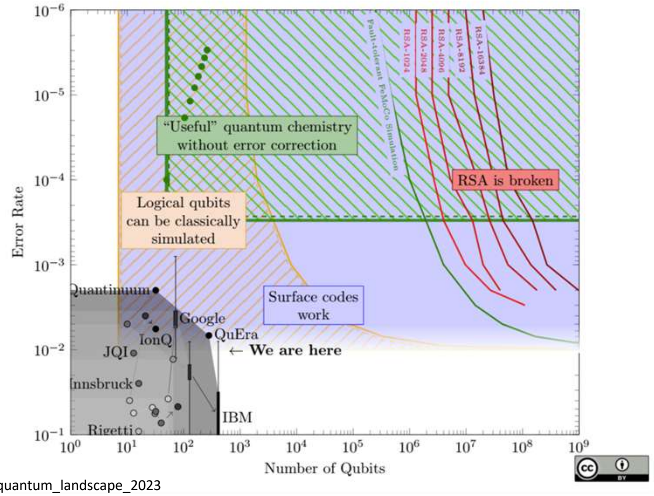


longer coherence times mean lower error rates
which allows more time to compute

IBM Quantum Experience – http://quantumexperience.ng.bluemix.net/

© 2017 IBM

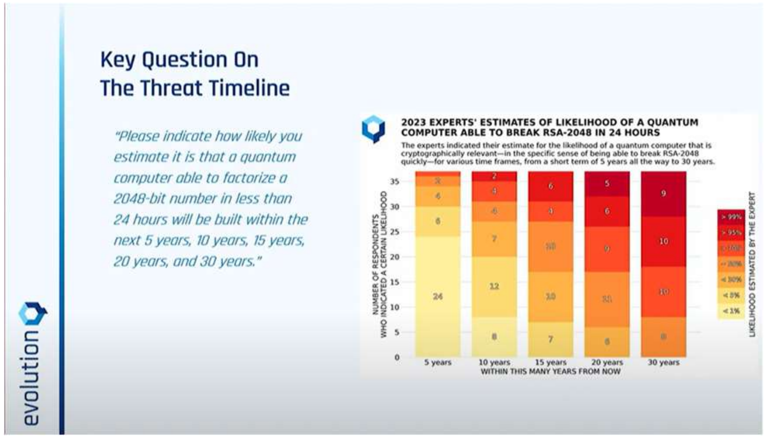
14



https://sam-jaques.appspot.com/quantum_landscape_2023

15

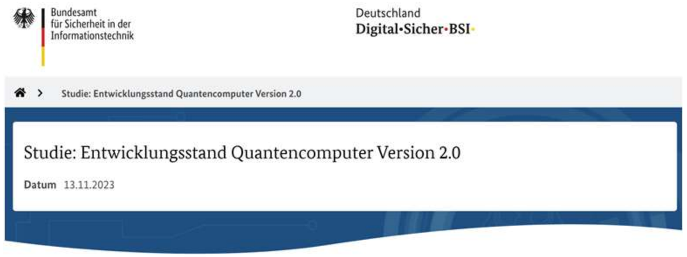
What do "the experts" say? (2023)



Source: Michele Mosca - https://www.youtube.com/watch?v=iZmWTkG64Xo

16

What does BSI say?



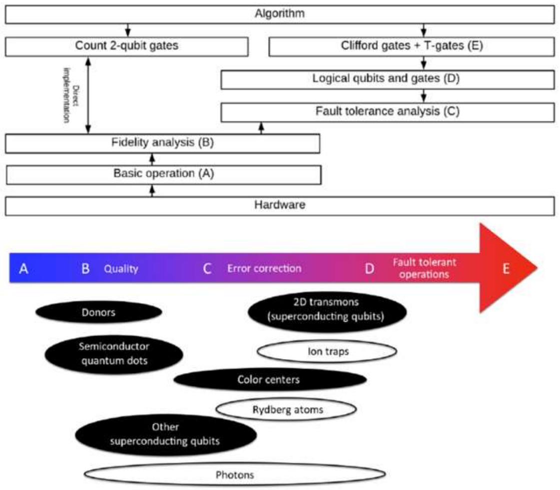
Noisy Intermediate-Scale Quantum (NISQ): due to the unknown scaling of these algorithms and based on larger theoretical arguments it is not likely that cryptanalytic quantum advantage can be reached in the NISQ domain.

Cryptographically Relevant Quantum Computers (QRQC): superconducting system with the surface code or an ion-based system with the color code will take at least one decade, more likely two. But surprises are possible.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_0.html 17

17

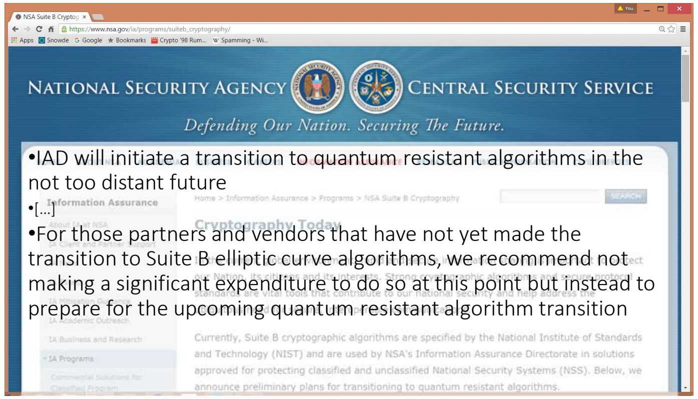
What does BSI say?



18

18

What did the NSA say? August 19 2015: do not switch to Suite B



- IAD will initiate a transition to quantum resistant algorithms in the not too distant future
- […]
- For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition

19

What do some other experts say?

The Register

You can cross 'Quantum computers to smash crypto' off your list of existential fears for 30 years

RSA's Adi Shamir thinks we're safe for a generation, but more gnarly keys are still a good idea

Iain Thomson Wed 26 Apr 2023 06:28 UTC

RSA CONFERENCE Adi Shamir, the cryptographer whose surname is the "S" in "RSA", thinks folks need to stop worrying about quantum computing breaking encryption algorithms.

Speaking on the annual cryptographers' panel at the RSA Conference in San Francisco this week, he opined that in the 1990s he saw three big issues appear on the security industry's radar: AI, cryptography, and quantum computing. Two out of three had delivered, he said, and quantum computing has yet to show promise and won't for decades to come.

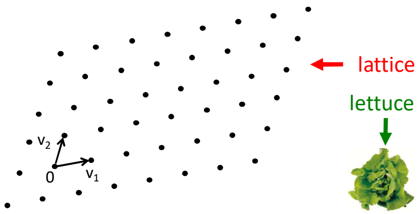
20

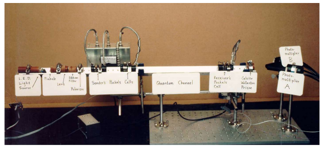
20

Post-quantum Cryptography ≠ Quantum Key Distribution

Find new cryptographic algorithms that resist attacks on quantum computers

Use quantum physics to agree on secret keys





Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

21

Post-Quantum Cryptography

- Go back to the 1970s
  - digital signatures based on one-way functions
  - public-key encryption based on Error Correcting Coding [McEliece'78] and extensions to rank metrics
  - public key encryption based on lattices (inspired by knapsack problems) (Euclidean distance)
- Go back to the 1980s:
  - Digital signatures based on multivariate polynomial equations

- Innovation from the 200s:
  - Isogenies of elliptic curves
- So far no good quantum algorithms known to break these systems

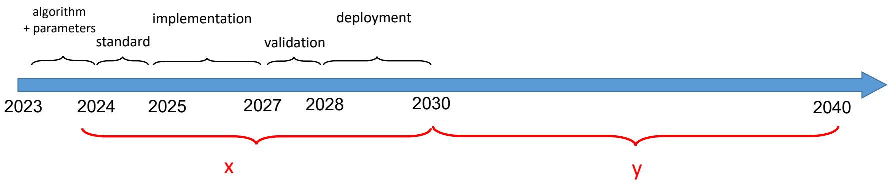
22

When to switch to post-quantum cryptography? [Mosca]

Q = #years until first large quantum computer
x = #years it takes to switch (3-12 years)
y = #years data needs to be confidential (10 years)

Need to start switching in the year 2024 + Q – x – y
e.g. Q = 16, x=7, y=10: today!

For digital signatures, y ≈ 0



23

NIST Post-Quantum Competition (2016-2026?)

https://en.wikipedia.org/wiki/Post-Quantum_Cryptography_Standardization
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Encryption: KYBER
Digital signatures: Dilithium, Falcon, SPHINCS+ (hash-based signature)

	Signatures	Encryption/KEM	TOTAL
Lattice	4/3/2/2	24/9/3/1	28/12/5/3
Code	5/0/0/0	19/7/1/0	24/7/1/0
Multivariate	7/4/1/0	6/0/0/0	13/4/1/0
Hash	4/1/0/1	0/0/0/0	4/1/0/1
Other	3/1/0/0	10/1/0/0	13/2/0/0
TOTAL	23/9/3/3	59/17/4/1	82/26/7/4

IETF (independent of NIST): 2 hash-based signatures
- RFC 8554 Leighton-Micali signatures
- RFC 8391 XMSS eXtended Merkle signatures

24

24

Evaluation Criteria

Security
- Security levels offered
- Confidence in proofs
- Attacks
- Classical/quantum complexity

Performance
- Size of parameters
- Speed of Keygen Enc/Dec
- Sign/Verify
- Software/hardware benchmarks

Algorithm and implementation
- IP issues
- Decryption failures
- Side channel resistance
- Simplicity and clarity of docs
- flexibility

Other
- Comments received
- Academic papers published

25

NIST: Winners and 4th round candidates

Family	Signatures	KEM / Encryption
Lattice-based	**Dilithium** **Falcon**	**Kyber** Saber NTRU FrodoKEM NTRUprime
Hash-based	**Sphincs+**	---
Code-based	---	Classic McEliece Bike HQC
Multivariate	~~GeMSS~~ Rainbow	---
Other	Picnic	SIKE

BSI and ANSSI (FrodoKEM)

BSI (Classic McEliece)

26

26

Cosic breaks two finalists

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

Wouter Castryck, Thomas Decru
Microsoft bounty of 50.000$

Paper 2022/214

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

27

27

NIST: Winners and 4th round candidates

Family	Signatures	KEM / Encryption
Lattice-based	**Dilithium** **Falcon**	**Kyber** Saber NTRU FrodoKEM NTRUprime
Hash-based	**Sphincs+**	---
Code-based	---	Classic McEliece Bike HQC
Multivariate	~~GeMSS~~ ~~Rainbow~~	---
Other	Picnic	~~SIKE~~

BSI and ANSSI (FrodoKEM)

BSI (Classic McEliece)

28

28

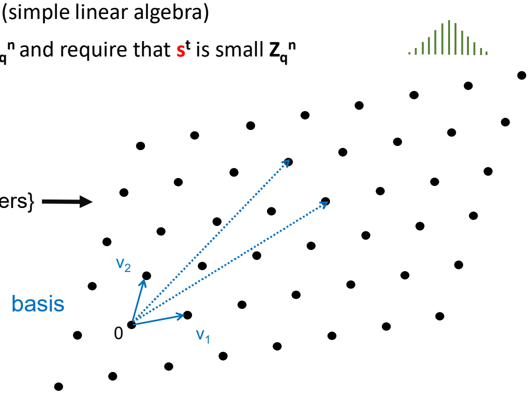
Learning With Errors (LWE)

- Consider mxn matrix $\mathbf{A} \in \mathbf{Z}_q^{mxn}$ and n-dimensional vectors $\mathbf{s}^t$, $\mathbf{b}^t \in \mathbf{Z}_q^n$
- Easy problem: solve $\mathbf{s}^t$ from $\mathbf{A} . \mathbf{s}^t = \mathbf{b}^t$ (simple linear algebra)
- Hard problem: add small noise $\mathbf{e}^t \in \mathbf{Z}_q^n$ and require that $\mathbf{s}^t$ is small $\mathbf{Z}_q^n$

$$\mathbf{A}\ \mathbf{s}^t = \mathbf{b}^t + \mathbf{e}^t$$

- Solutions $\mathbf{s}^t$, $\mathbf{e}^t$ form a shifted lattice

lattice $L=\{\mathbf{a}_1\mathbf{v}_1+\ldots+\mathbf{a}_n\mathbf{v}_n \mid \mathbf{a}_i \text{ integers}\}$ →




← lettuce

29

Learning with error variants: $\mathbf{A}\mathbf{s}^t = \mathbf{b}^t + \mathbf{e}^t$

Structure of A (warning: highly simplified)

2	3	4	7
5	6	2	1
9	8	5	2
4	2	3	9

random lattice

ciphertext, public key
10 Kbyte
Frodo encryption

2	3	4	7
3	2	7	4
9	8	5	2
8	9	2	5

module lattice

ciphertext, public key
1 Kbyte
Kyber encryption
Dilithium signature
signature 2.7 Kbyte
public key 1.2 Kbyte

2	3	4	7
7	2	3	4
4	7	2	3
3	4	7	2

ideal lattice (ring)

ciphertext, public key
< 1 Kbyte

30

30

"Diffie-Hellman" lattice variant based on Learning With Errors (LWE) [Ding+12] simplified

Public parameters: prime q and matrix $\mathbf{A} \in \mathbf{Z}_q^{nxn}$

Alice chooses small $\mathbf{s}_A$ and $\mathbf{e}_A \in \mathbf{Z}_q^n$

computes $\mathbf{p}_A = \mathbf{A}\ \mathbf{s}_A^t + \mathbf{e}_A^t \bmod q$ and sends this to Bob

Bob chooses small $\mathbf{s}_B$ and $\mathbf{e}_B \in \mathbf{Z}_q^n$

computes $\mathbf{p}_B = \mathbf{A}\ \mathbf{s}_B^t + \mathbf{e}_B^t \bmod q$ and sends this to Alice

Alice computes $\mathbf{s}_A\ \mathbf{p}_B$ and Bob computes $\mathbf{s}_B\ \mathbf{p}_A$

Note that $\mathbf{s}_A\ \mathbf{p}_B \approx \mathbf{s}_B\ \mathbf{p}_A \approx \mathbf{s}_B\ \mathbf{A}\ \mathbf{s}_A^t$ but some error correction needed

Slide credit: Frederik Vercauteren

31

Connection LWE with lattices

Given vector $\mathbf{b} \in \mathbf{Z}_q^{nx1}$ and matrix $\mathbf{A} \in \mathbf{Z}_q^{nxn}$ with $\mathbf{b} = \mathbf{A}\ \mathbf{s} + \mathbf{e}$

Errors are "small" when reduced in the interval [-q/2,q/2]

Natural definition of smallness

Consider the set of vectors in $\mathbf{Z}_q^{mx1}$

$\Lambda(\mathbf{A}) = \{ \mathbf{z} \in \mathbf{Z}_q^{mx1} \mid \mathbf{z} = \mathbf{A}.\mathbf{x} \bmod q \text{ and } \mathbf{x} \in \mathbf{Z}_q^n \}$

$\Lambda(\mathbf{A})$ forms a lattice; indeed if $\mathbf{z}_1, \mathbf{z}_2 \in \Lambda(\mathbf{A})$ then $\mathbf{z}_1 - \mathbf{z}_2 \in \Lambda(\mathbf{A})$

If $\mathbf{e} \neq 0$ but small, then $\mathbf{b} \notin L(\mathbf{A})$ but still quite close to it

Solving Bounded Distance Decoding (distance d) with $d > ||\mathbf{e}||$ removes errors

Slide credit: Frederik Vercauteren

32

Key Aspects of Lattice-based Systems

Pros

- efficient and parallizable
  - matrix-vector arithmetic, Fast-Fourier Transform for polynomial multiplication
- worst-case to average-case reductions

Cons

- difficult to find good sampling methods
- difficult to assess exact security
- large keys (except for ring, module and NTRU versions)
- probabilistic decryption

33

Digital signatures

	PQ	Size (Bytes)		CPU time (lower is better)	
		Public Key	Signature	Signing	Verification
Dilithium2	Y	1,312	2,420	4,8	0,5
Falcon512	Y	897	666	8*	0,5
Sphincs+ (speed)	Y	32	17,088	550	7
Sphincs+ (size)	Y	32	7,856	8,000	2,8
RSA-2048	N	256	256	70	0,3
Ed25519	N	32	64	1 (baseline)	1 (baseline)

Disclaimer: numbers by Cloudflare, should be used with caution. These numbers vary considerably for different platforms and implementations. Should only be used as rough guideline.

Source: https://blog.cloudflare.com/nist-post-quantum-surprise/

34

34

Dilithium vs. Falcon

+ Security reasonably well understood
+ Efficient
- Larger key sizes than pre-quantum

Dilithium

- Simple
- Large bandwidth (2420 bytes)
- NIST Standard Summer '24

Falcon

- Complicated
  - Floating point arithmetic
  - Specification unclear
- Medium bandwidth (660 bytes)
- Very efficient with floating point
- NIST Standard Summer'25??

35

35

Hash-based signatures

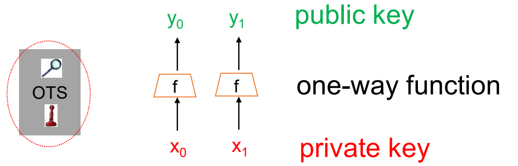
- **NIST: Sphincs+ (stateless)**
  - Large (x100 vs pre-quantum)
  - Slow (x500 vs pre-quantum)
  - Alternative to lattice-based
  - Security very well understood
- **IETF (stateful)**
  - RFC 8554 Leighton-Micali signatures
  - IETF RFC 8391 XMSS eXtended Merkle
    - x30 faster than Sphincs+
    - But additional constraints on sender and receiver staying in sync

36

36

Hash-Based Signatures: Lamport One-Time Signature (1979)

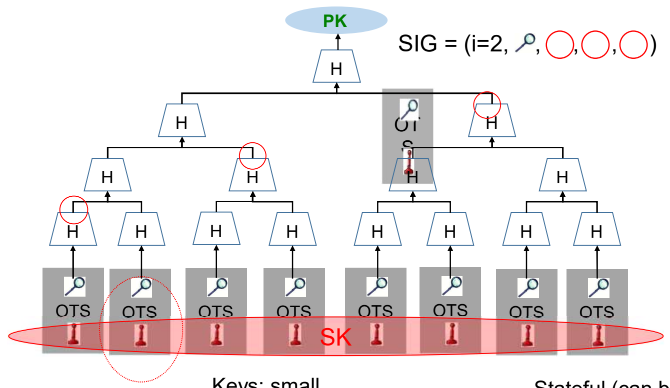
SIG = (x_1)



Slide credit: Andreas Hülsing

37

Hash-Based Signatures: Merkle trees



Keys: small
Signature size: medium
Verification/signature: slow

Stateful (can be a problem)
Stateless variants: slower

Slide credit: Andreas Hülsing

38

Digital signatures: next steps

- NIST launched call for proposals in other families
  - Multivariate crypto
    - Large key (Rainbow x100 vs Dilithium)
    - Small signature (Rainbow x0.03 vs Dilithium)
    - Slower (Rainbow x20 vs Dilithium)

- Summer'23: 40 candidates that met all submission requirements

39

39

Security levels

Level	Classical	
I	AES 128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
II	SHA3-256	2^{146} classical gates
III	AES192	2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates
IV	SHA3-384	2^{210} classical gates
V	AES256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates

Criticism: too vague
- circuit depth
- cost of memory
- which quantum gates?

40

40

Same API

- Key Generation, Encryption, Decryption
- Key Generation, Signing, Verification

41

41

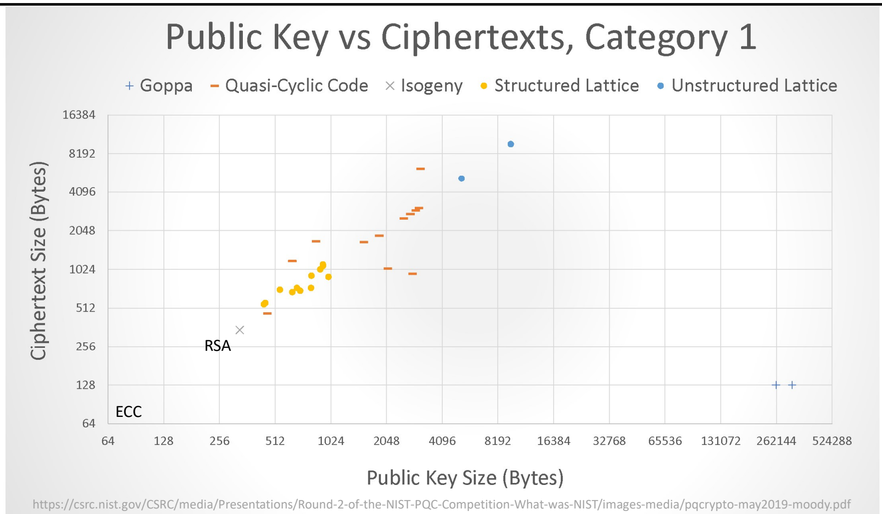
Benchmarking initiatives

- Microprocessor (Cortex M4) code and benchmark:
  - https://github.com/mupq/pqm4
- Standalone implementations:
  - https://github.com/PQClean/PQClean
  - Benchmarked here: https://bench.cr.yp.to/supercop.html

This is academic and not industrial grade code! Use with caution.

42

42



43

Encryption / KEM comparison

	Size (Bytes)		Ops/sec (Higher is better)		
	Public Key	Ciphertext	Keygen	Encaps / Encrypt	Decaps / Decrypt
Kyber-512	800	768	125,000	80,000	100,000
RSA-2048	256	256	30	150,000	1,400
ECC X25519	64	64	80,000	15,000	19,000

Disclaimer: numbers by Cloudflare, should be used with caution. These numbers vary considerably for different platforms and implementations. Should only be used as rough guideline.

Source: https://blog.cloudflare.com/nist-post-quantum-surprise/

44

44

Encryption / KEM comparison

- Kyber only standard (for now)
  - + Security reasonably well understood
  - + Efficient
  - - Larger key sizes than pre-quantum
- NIST launched call for proposals in other families (round 4)
  - Code-based cryptography
  - + Reasonably efficient (e.g. BIKE x10 vs Kyber)
  - - Similar sizes to Kyber (e.g. BIKE x2 vs Kyber)

45

45

NIST Post-Quantum Standardization Effort

http://csrc.nist.gov/pqcrypto

Fall 2016		Formal call for proposals – NISTIR 8105
July 2022	4	Winners announced batch 1
Sep. 2022		Call for new digital signature schemes
Oct. 2022	3	Start of Round 4: BIKE, Classic McEliece, HQC, ~~SIKE~~
Jun. 2023		Deadline for submitting new signature schemes
Summer 2023		Release draft standard batch 1 (Falcon only late 2024)
Summer 2024		Parameters batch 1 chosen and standard published
2024		End of Round 4?
2025?		Selection of new signature schemes
2026?		Additional standards published

46

How to continue?

- Pre-Quantum era
  - RSA / ECC
- Hybrid era
  - RSA / ECC + Post-Quantum

	OR: gradual transition	AND: no gradual transition
Digital signature	Ok	Long term secure
Public key encryption	No long term security	Long term secure

- Post-Quantum Era
  - Once confidence in post-quantum is high enough

PKI migration will be challenging due to complexity and increased size of certificates (size of signature + public key)

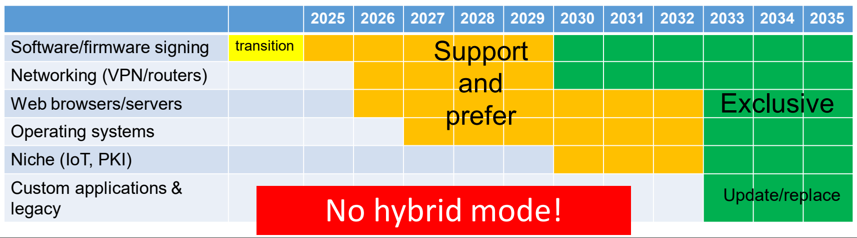
47

47

What did the NSA say in Sept.'22?

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

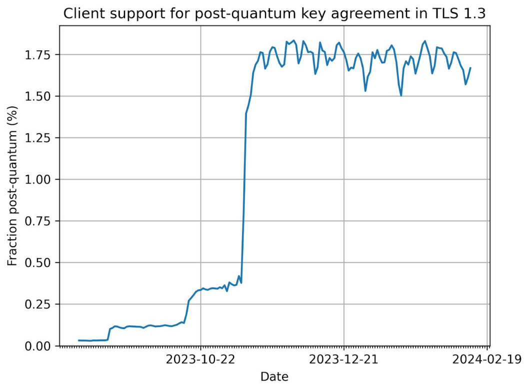
AES-256, SHA-384, SHA-512
LMS/XMSS
CRYSTALS-Kyber, CRYSTALS-Dilithium level V



48

Cloudflare Blog Post (May'24)

https://blog.cloudflare.com/pq-2024



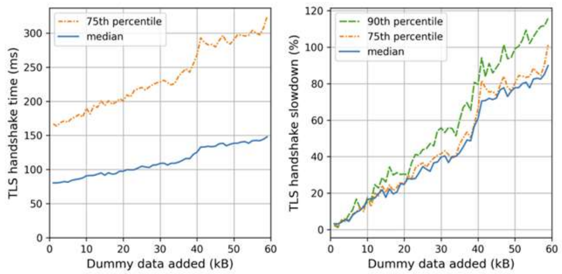
Early '24

Late '24

49

49

TLS slowdown (source: Cloudflare)



Performance when artificially inflating certificate chain size to simulate post-quantum certificates.

50

50

Cryptographic governance

- Understanding where crypto is being used by building an **Inventory**:
- **Monitoring** crypto is being used
- **Auditing** that crypto is being used in accordance with a specific standard, regulations or policy
- The **enforcement** of minimum security policy for crypto usage
- Policy for **migration** to new generations of cryptography
- Policy for the **retirement** of older cryptography
- Managing cryptography used in **supply chains**, provided by third parties
- Policy to **consolidate** and **simplify** an Enterprise crypto landscape
- Guidance on how applications should consume cryptography to allow simpler migration of cryptographic (**cryptographic agility**):
- Lack of **strategic interlock** with new application and application migration
- Guidance on **deployment models** for hybrid cloud platforms

Source: IBM Quantum

51

51

OWASP Top 10

https://www.owasp.org/Top10

1. Broken access control
2. Cryptographic failures (Data Breach)
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

No Encryption
Weak Algorithms
Default Keys
Cryptographic Usage
Certificate management
Security Configuration
Use of Randomness
………

52

52

OWASP Top 10

https://www.owasp.org/Top10

1. Broken access control
2. Cryptographic failures (Data Breach)
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

All rely on public key cryptography!

53

53

National Cybersecurity Center of Excellence (NCCoC) (US): pragmatic approach (missing in EU)

- NIST Special Publication 800-38A: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography
- Coordination
- Automated tools for detection of cryptographic libraries
- Interoperability and performance demonstrations across different technology and protocols to include TLS, QUIC, SSH, code signing, public key certificates, hardware security modules, etc.
- https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-postquantum-cryptographic-algorithms

54

54

Some applications will migrate to pure symmetric cryptography or will add this as backup

- Computationally secure: most likely
  - Performance is excellent (AES < 1 cycle/byte)
  - Always online: fine today
  - To trusted center: problematic but threshold systems may work
  - Or hardware assumption
- Information theoretic security for some applications
  - one-time pad + unconditionally secure MAC algorithm

55

55

Challenges: technical

- Slow process
- Larger keys/ciphertexts/signatures
- Most robust schemes have worse performance: hash-based signature and Classic McEliece
- Lattice based schemes
  - Good performance
  - Some uncertainty about parameters for structured lattices
  - Decryption failure, floating point, noise sampling
- Side channel resistance: KyberSlash, KEM in Fujisaki-Okamoto mode: FO-calyps

[Azouaoui et al., Surviving the FO-CALYPS: Securing PQC Implementations in Practice, RWC'22]

56

56

Challenges: other

- Upgrading is slow
- Upgrading is expensive
- Long term problem
- PKI: middleboxes and clients break when certificate chains grow by 10kB/30kB

Need regulation: strategic EU approach for 2026 (3 years behind)

https://www.nldigitalgovernment.nl/news/new-eu-recommendation-on-post-quantum-cryptography/

New EU Recommendation on Post-Quantum Cryptography

On 11 April 2024, the European Commission published a recommendation regarding the transition to Post-Quantum Cryptography (PQC).

57

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN
ArenBerg Crypto BV
COSIC

58

McEliece security notions

Private key security
Relies on the difficulty of retrieving inner code from public matrix *H* and thus getting access to efficient decoding

Message security
decryption security relies on NP-hardness of the syndrome-decoding problem for a random code - assuming that structure of *H* does not leak (best known algorithms take exponential time)

Public key is large random matrix *H*

Syndrome decoding problem: find vector e of Hamming weight t that solves this equation

								e		s
0	1	1	0	1	...	0		0		0
1	1	0	1	0	...	1		1		0
1	1	1	0	0	...	1		0		1
0	0	1	1	0	...	0		0	=	1
1	1	1	0	1	...	1		0		0
...	...	...	...	...	...	...		...		...
0	1	0	1	1	...	0		1		1
1	1	1	0	1	...	1		0		1

59

McEliece: suitable codes don't have too much structure

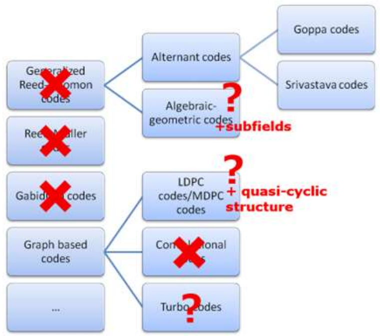
McEliece's original proposal (1978) Goppa codes is still holding up

large key sizes: 187 kB for 128-bit security

Need to randomize plaintext!

Small ciphertexts

Recently: rank codes



60

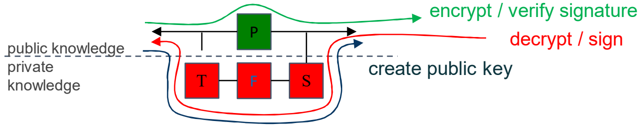
Multivariate Quadratic Equations ('88)

$$y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3$$
$$y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1$$
$$y_3 = \dots$$

Public Key:
- system of quadratic polynomials P : $F_q^n \rightarrow F_q^m$

Private Key:
- affine transformations T : $F_q^m \rightarrow F_q^m$ (on output variables) and S : $F_q^n \rightarrow F_q^n$ (on input variables)
- central system of quadratic polynomials F : $F_q^n \rightarrow F_q^m$ (easily invertible)

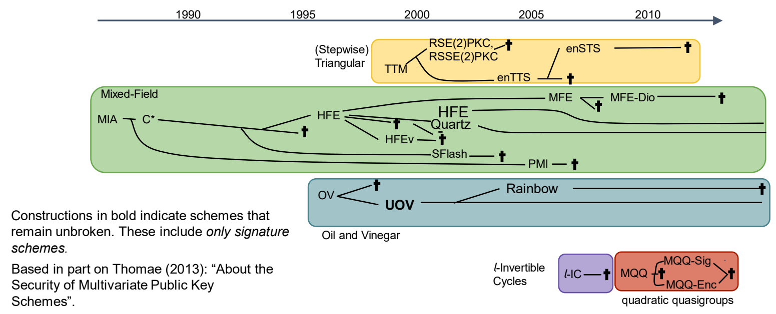
S and T hide the structure of F: P = T ∘ F ∘ S



Slide credit: Alan Szepeniec

61

Multivariate Quadratic Equations



Slide credit: Alan Szepeniec

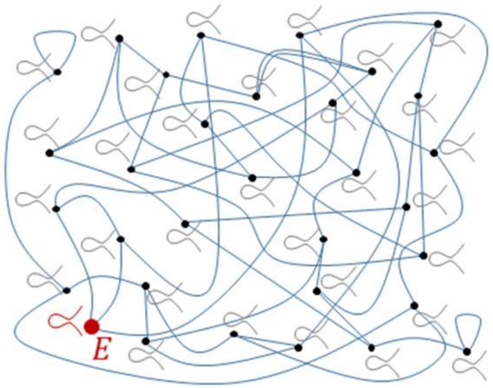
62

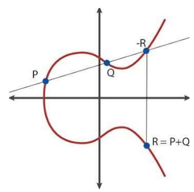
Codes, Lattices and MQ

- Allow (in theory) both KEM and digital signatures
- Average-case versions of NP-hard problems
- Best known quantum attacks (so far): "Quantizations" of classical attacks
- Need "structured versions" for efficiency: security implications?
- Theoretically, signatures & KEM possible

63

Isogenies: SIKE





$y^2 = x^3 + ax + b \bmod p$

Slide credit: Wouter Castryck

64

64